Image Encryption Using Advanced Hill Cipher Algorithm

Bibhudendra Acharya[1], Saroj Kumar Panigrahy[2], Sarat Kumar Patra[3], and Ganapati Panda[3]
[1]Department of E & TC, NIT Raipur, Chhattisgarh-492010, India
bibhudendra@gmail.com
[2]Department of CSE, NIT Rourkela, Orissa-769008, India
skp.nitrkl@gmail.com
[3]Department of ECE, NIT Rourkela, Orissa-769008, India
{skpatra, gpanda}@nitrkl.ac.in

***Abstract*—The Hill cipher algorithm is one of the symmetric key algorithms that have several advantages in data encryption. But, the inverse of the key matrix used for encrypting the plaintext does not always exist. Then if the key matrix is not invertible, then encrypted text cannot be decrypted. In the Involutory matrix generation method the key matrix used for the encryption is itself invertible. So, at the time of decryption we need not to find the inverse of the key matrix. The objective of this paper is to encrypt an image using a technique different from the conventional Hill Cipher. In this paper a novel advanced Hill (AdvHill) encryption technique has been proposed which uses an involutory key matrix. The scheme is a fast encryption scheme which overcomes problems of encrypting the images with homogeneous background. A comparative study of the proposed encryption scheme and the existing scheme is made. The output encrypted images reveal that the proposed technique is quite reliable and robust.**

***Index Terms*—Encryption, Decryption, Hill Cipher, Image Encryption, Advanced Hill Cipher.**

I. Introduction

Owing to the advance in network technology, information security is an increasingly important problem. Popular application of multimedia technology and increasingly transmission ability of network gradually leads us to acquire information directly and clearly through images. Cryptography, the science of encryption, plays a central role in mobile phone communications, pay-TV, e-commerce, sending private emails, transmitting financial information, security of ATM cards, computer passwords, and touches on many aspects of our daily lives. Cryptography is the art or science encompassing the principles and methods of transforming an intelligible message (plaintext) into one that is unintelligible (ciphertext) and then retransforming that message back to its original form. In modern times, cryptography is considered to be a branch of both mathematics and computer science, and is affiliated closely with information theory, computer security, and engineering [1].

Substitution cipher is one of the basic components of classical ciphers. A substitution cipher is a method of encryption by which units of plaintext are substituted with ciphertext according to a regular system; the units may be single letters (the most common), pairs of letters, triplets of letters, mixtures of the above, and so forth. The receiver deciphers the text by performing an inverse substitution [8]. The units of the plaintext are retained in the same sequence as in the ciphertext, but the units themselves are altered. There are a number of different types of substitution cipher. If the cipher operates on single letters, it is termed a simple substitution cipher; a cipher that operates on larger groups of letters is termed polygraphic. A monoalphabetic cipher uses fixed substitution over the entire message, whereas a polyalphabetic cipher uses a number of substitutions at different times in the message— such as with homophones, where a unit from the plaintext is mapped to one of several possibilities in the ciphertext. Hill cipher is a type of monoalphabetic polygraphic substitution cipher. Hill cipher is a block cipher that has several advantages such as disguising letter frequencies of the plaintext, its simplicity because of using matrix multiplication and inversion for enciphering and deciphering, its high speed, and high throughput [5,7].

In this paper, we have proposed an advanced Hill (AdvHill) cipher algorithm which uses an Involutory key matrix for encryption [1]. The objective of this paper is to overcome the drawback of using a random key matrix in Hill cipher algorithm for encryption, where we may not be able to decrypt the encrypted message, if the key matrix is not invertible. Also the computational complexity can be reduced by avoiding the process of finding inverse of the matrix at the time of decryption, as we use Involutory key matrix for encryption. Using this key matrix we encrypted gray scale as well as color images. Our algorithm works well for all types of gray scale as well as color images except for the images with background of same gray level or same color.

The organization of the paper is as follows. Following the introduction, the basic concept of Hill Cipher is outlined in section II. Section III discusses about the modular arithmetic. In section IV, a method of generating

This research work was carried out at the Department of ECE, NIT Rourkela, Orissa-769008, India.
Corresponding author: bibhudendra@gmail.com

© 2010 ACEEE
DOI: 01.ijsip.01.01.08

Involutory key matrix is explained. Section V presents the proposed method of image encryption using advanced Hill Cipher (AdvHill) algorithm. Experimental results are discussed in section VI. Finally, section VII describes the concluding remarks.

II. HILL CIPHER

It is developed by the mathematician Lester Hill. The core of Hill cipher is matrix manipulations. For encryption, algorithm takes m successive plaintext letters and instead of that substitutes m cipher letters. In Hill cipher, each character is assigned a numerical value like $a = 0, b = 1, \ldots, z = 25$ [5, 9]. The substitution of ciphertext letters in the place of plaintext letters leads to m linear equation. For $m = 3$, the system can be described as follows:

$$\begin{aligned} C_1 &= (K_{11}P_1 + K_{12}P_2 + K_{13}P_3) \bmod 26 \\ C_2 &= (K_{21}P_1 + K_{22}P_2 + K_{23}P_3) \bmod 26 \\ C_1 &= (K_{31}P_1 + K_{32}P_2 + K_{33}P_3) \bmod 26 \end{aligned} \quad \ldots (1)$$

This case can be expressed in terms of column vectors and matrices:

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{bmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{bmatrix} \begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} \quad \ldots (2)$$

or simply we can write as $C = KP$, where C and P are column vectors of length 3, representing the plaintext and ciphertext respectively, and K is a 3×3 matrix, which is the encryption key. All operations are performed mod 26 here. Decryption requires using the inverse of the matrix K. The inverse matrix K^{-1} of a matrix K is defined by the equation $KK^{-1} = K^{-1}K = I$, where I is the Identity matrix. But the inverse of the matrix does not always exist, and when it does, it satisfies the preceding equation. K^{-1} is applied to the ciphertext, and then the plaintext is recovered [2,6]. In general term we can write as follows:

For encryption:

$$C = E_k(P) = K_p \quad \ldots (3)$$

For decryption:

$$P = D_k(C) = K^{-1}C = K^{-1}K_p = P \quad \ldots (4)$$

If the block length is m, there are 26^m different m letters blocks possible, each of them can be regarded as a letter in a 26^m-letter alphabet. Hill's method amounts to a monoalphabetic substitution on this alphabet [5].

III. MODULAR ARITHMETIC

The arithmetic operation presented here are addition, subtraction, unary operation, multiplication and division [9]. Based on this, the Involutory matrix for Hill cipher algorithm is generated. The congruence modulo operator has the following properties:

1. $a \equiv b \mod p$ if $n \mid (a - b)$
2. $(a \bmod p) = (b \bmod p) \Rightarrow a \equiv b \bmod p$
3. $a \equiv b \bmod p \Rightarrow b \equiv a \bmod p$
4. $a \equiv b \bmod p$ and $b \equiv a \bmod p \Rightarrow a \equiv c \bmod p$

Let $Z_p = [0, 1, \ldots, p - a]$ the set of residues modulo p. If modular arithmetic is performed within this set Z_p, the following equations present the arithmetic operations:

Addition:

$$(a + b) \bmod p = [(a \bmod p) + (b \bmod p)] \bmod p$$

Negation:

$$-a \bmod p = p - (a \bmod p)$$

Subtraction:

$$(a - b) \bmod p = [(a \bmod p) - (b \bmod p)] \bmod p$$

Multiplication:

$$(a * b) \bmod p = [(a \bmod p) * (b \bmod p)] \bmod p$$

Division:

$$(a / b) \bmod p = c \text{ when } a = (b * c) \bmod p$$

The following exhibits the properties of modular arithmetic.

Commutative Law:

$$(\omega + x) \bmod p = (x + \omega) \bmod p$$
$$(\omega * x) \bmod p = (x * \omega) \bmod p$$

Associative law:

$$[(\omega + x) + y] \bmod p = [\omega + (x + y)] \bmod p$$

Distribution Law:

$$[\omega * (x + y)] \bmod p = [\{(\omega * x) \bmod p\} * \{(\omega * y) \bmod p\}] \bmod p$$

Identities:

$$(0 + a) \bmod p = a \bmod p$$
$$\text{and } (1 * a) \bmod p = a \bmod p$$

© 2010 ACEEE
DOI: 01.ijsip.01.01.08

Inverses:

For each $x \in Z_p$, $\exists y$ such that

$(x+y) \bmod p = 0$ then $y = -x$

For each $x \in Z_p$ $\exists y$ such that $(x * y) \bmod p = 1$

IV. Generation of Involutory Key Matrix

The proposed AdvHill algorithm uses an involutory key matrix for encryption technique. The various proposed methods can be found in literature [1]. One of the methods is explained below.

A is called a involutory matrix if $A = A^{-1}$. The analysis presented here for generation of involutory key matrix is valid for matrix of +ve integers that are the residues of modulo arithmetic of a number. This algorithm can generate involutory matrices of order $n \times n$ where n is even.

Let $A=\begin{bmatrix} a_{11} & a_{12} & \dots & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & \dots & a_{2n} \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & \dots & a_{nn} \end{bmatrix}$ be an $n \times n$ involutory matrix partitioned to $A=\begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix}$, where n is even and A_{11}, $A_{12,}A_{21}$ & A_{22} are matrices of order $\frac{n}{2} \times \frac{n}{2}$ each.

So, $A_{12}A_{21} = I - A_{11}^2 = (I - A_{11})(I + A_{11})$

If A_{12} is one of the factors of $I - A_{11}^2$ then A_{21} is the other.

Solving the 2nd matrix equation results $A_{11} + A_{22} = 0$.

Then form the matrix.

Algorithm:

1. Select any arbitrary $\frac{n}{2} \times \frac{n}{2}$ matrix A_{22}.
2. Obtain $A_{11} = -A_{22}$.
3. Take $A_{12} = k(I - A_{11})$ or $k\ (I + A_{11})$ where k is a scalar constant.
4. Then, $A_{21} = \frac{1}{k}(I + A_{11})$ or $\frac{1}{k}(I - A_{11})$.

5. Form the matrix completely.

Example: (For Modulo 13)

Let $A_{22} = \begin{bmatrix} 10 & 2 \\ 3 & 4 \end{bmatrix}$,

then, $A_{11} = \begin{bmatrix} 3 & 11 \\ 10 & 9 \end{bmatrix}$.

If k is selected as 2,

then, $A_{12} = k(I - A_{11}) = \begin{bmatrix} 9 & 4 \\ 6 & 10 \end{bmatrix}$,

and $A_{21} = \begin{bmatrix} 2 & 12 \\ 5 & 5 \end{bmatrix}$

So, $A = \begin{bmatrix} 3 & 11 & 9 & 4 \\ 10 & 9 & 6 & 10 \\ 2 & 12 & 10 & 2 \\ 5 & 5 & 3 & 4 \end{bmatrix}$ will be the involutory matrix.

V. Image Encryption using AdvHill Technique

As we note that Hill cipher can be adopted to encrypt grayscale and color images, proposed AdvHill algorithm can also be used for grayscale and color images. For grayscale images, the modulus will be 256 (the number of levels is considered as the number of alphabets). In the case of color images, first decompose the color image into (R-G-B) components. Second, encrypt each component (R-G-B) separately by the algorithm. Finally, concatenate the encrypted components together to get the encrypted color image [10]. The algorithm is given below and the block diagram for the encryption process is shown in Figure 1.

Algorithm AdvHill:

Step1. A involutory key matrix of dimensions $m \times m$ is constructed.

Step2. The plain image is divided into $m \times m$ symmetric blocks.

Step3. The ith pixels of each block are brought together to form a temporary block.

a. Hill cipher technique is applied onto the temporary block.

b. The resultant matrix is transposed and Hill cipher is again applied to the this matrix.

Step4. The final matrix obtained is placed in the i^{th} block of the encrypted image.

© 2010 ACEEE
DOI: 01.ijsip.01.01.08

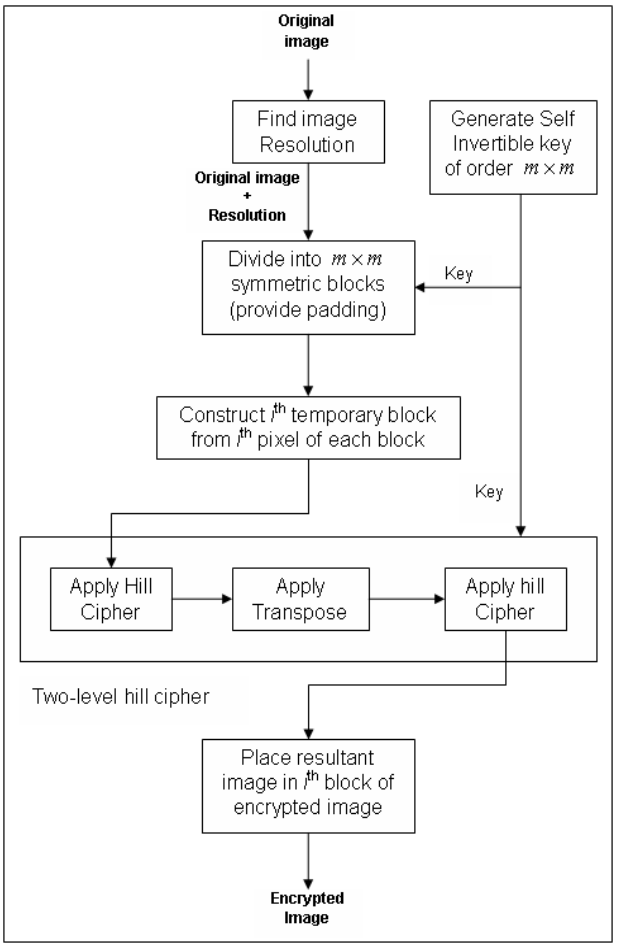

Figure. 1. The block diagram for proposed AdvHill algorithm.

VI. Experimental Results

We have taken different images and encrypted them using original Hill and our proposed AdvHill algorithm and the results are shown below in Figure 2 and 3. It is clearly noticeable from the Figure 2(e, g), that original Hill Cipher can't encrypt the images properly if the image consists of large area covered with same colour or gray level [8]. But our proposed algorithm works for any images with different gray scale as well as colour images. In Figure 3, it is found that our proposed AdvHill algorithm can able to encrypt the image properly as compared to original Hill Cipher algorithm.

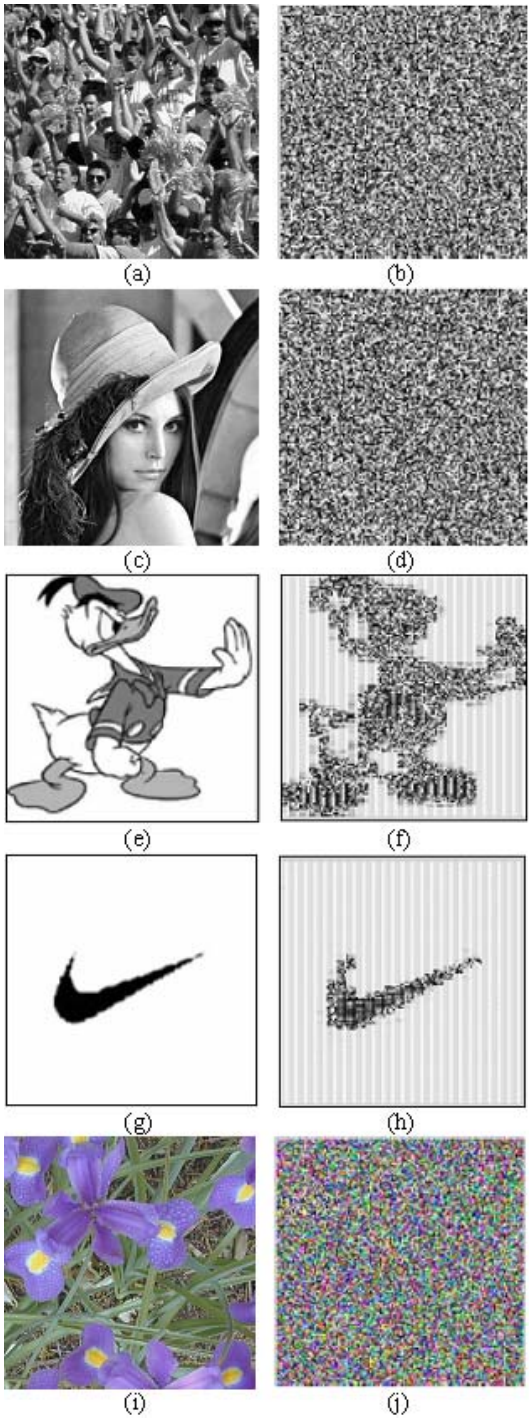

Figure. 2. Original images (a, c, e, g, i) and corresponding encrypted images (b, d, f, h, j) by original Hill Cipher Algorithm

© 2010 ACEEE
DOI: 01.ijsip.01.01.08

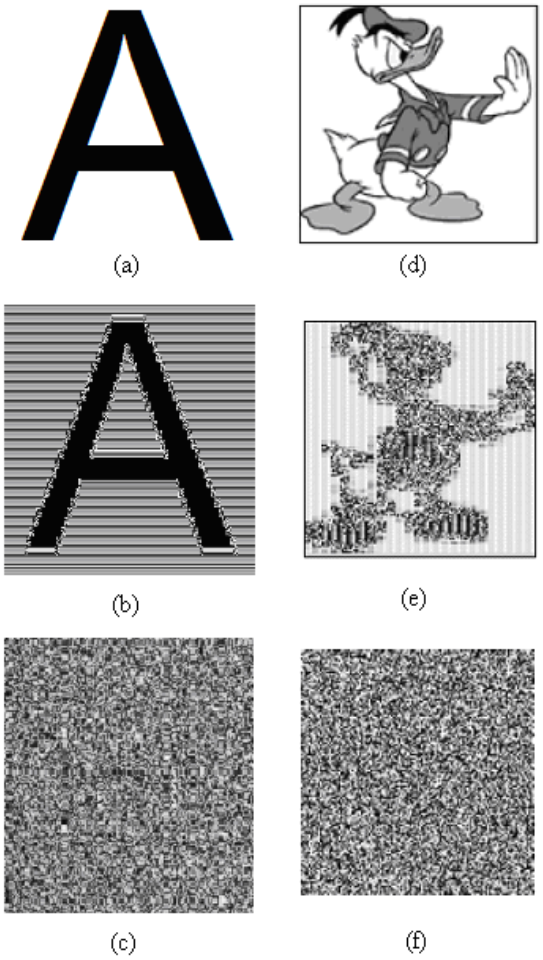

Figure. 3. Original images (a,d) and corresponding encrypted images (b,e) by original Hill Cipher Algorithm and (c,f) by our proposed AdvHill algorithm

VII. CONCLUSION

This paper suggests efficient method of encryption of image. Proposed AdvHill algorithm is more secure to brute force attacks as compared to original Hill cipher algorithm. A Brute Force Attack requires $2^{7+8*(n/2)^2}$ number of key generations; where n is the order of key matrix. AdvHill is a fast encryption technique which can provide satisfactory results against the normal hill cipher technique. The proposed scheme is resistant against known plaintext attacks.

REFERENCES

[1] Bibhudendra Acharya, Girija Sankar Rath, Sarat Kumar Patra, Saroj Kumar Panigrahy. 2007. Novel Methods of Generating Self-Invertible Matrix for Hill Cipher Algorithm, *International Journal of Security*, Vol 1, Issue 1, 2007, pp. 14-21.

[2] Imai H., Hanaoka G., Shikata J., Otsuka A., Nascimento A.C. 2002. Cyptography with Information Theoretic Security. Information Theory Workshop, 2002, Proceedings of the IEEE, 20-25 Oct 2002.

[3] Lerma, M.A., 2005. Modular Arithmetic. http://www.math.northwestern.edu/~mlerma/problem_solving/results/modular_arith.pdf.

[4] Li, S., Zheng, X., 2002. On the Security of an Image Encryption Method. ICIP2002. http://www.hooklee.com/Papers/ICIP2002.pdf.

[5] Menezes, A. J., P.C. Van Oorschot, S.A. Van Stone. 1996. Handbook of Applied Cryptography. CRC press.

[6] Overbey, J., Traves, W., Wojdylo, J., 2005. On the keyspace of the Hill cipher. *Cryptologia*, 29(l):59-72.

[7] Petersen, K., 2000. Notes on Number Theory and Cryptography.

http://www.math.unc.edu/Faculty/petersen/Coding/cr2.pdf.

[8] Saeednia, S., 2000. How to make the Hill cipher secure. *Cryptologia*, 24(4):353-360.

[9] Stallings, W. Cryptography and Network Security.2005. 4th edition, Prentice Hall.

[10] ISMAIL I.A., AMIN Mohammed, DIAB Hossam, How to repair the Hill cipher, *Journal of J Zhejiang Univ SCIENCE* A, vol. 7(12), pp. 2022-2030, 2006.

[11] Y. Rangel-Romero, R. Vega-García, A. Menchaca-Méndez, D. Acoltzi-Cervantes, L. Martínez-Ramos, M. Mecate-Zambrano, F. Montalvo-Lezama, J. Barrón-Vidales, N. Cortez-Duarte, F. Rodríguez-Henríquez, Comments on How to repair the Hill cipher, *Journal of J Zhejiang Univ SCIENCE* A, pp. 1-4, 2007.

© 2010 ACEEE
DOI: 01.ijsip.01.01.08

ACEEE